北京大学
PEKING UNIVERSITY

区块链技术原理、安全风险与创新

北京大学软件安全研究小组

目录

MORESHI POWERPOINT

区块链简介

MORESHI POWERPOINT

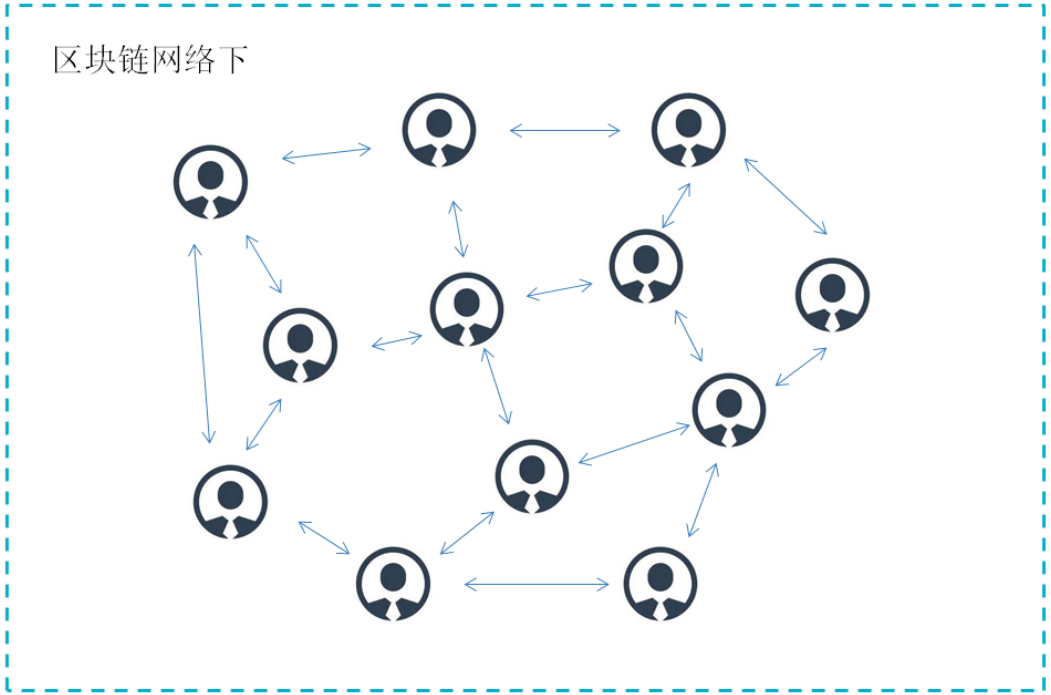
- 区块链是通过密码学的方式形成的一个由集体维护的分布式数据库。

区块链简介

MORESHI POWERPOINT

- 传统中心化的方式

- 区块链方式



区块链节点的架构

MORESHI POWERPOINT

“账本”

MORESHI POWERPOINT

现 金 日 记 账

年 月	日	凭证编号	摘要	对方科目编码	借方 千	百	十	万	千	百	十	元	角	分	√	贷方 千	百	十	万	千	百	十	元	角	分	√	余额 千	百	十	万	千	百	十	元	角	分

区块结构

MORESHI POWERPOINT

区块高度：可以理解为每个区块的唯一ID，从零开始的“创世块”（即块高度为0），一段时间生成一个块，块高度加1。

头哈希：每一个区块都有一个唯一哈希值，依据上一个区块的头哈希+数据块哈希+随机数生成

父哈希：上一个高度区块的哈希值

merkle根：区块中每一笔交易对应一个哈希，呈树状结构，生成的最终值（根），代表了该区块中的交易。

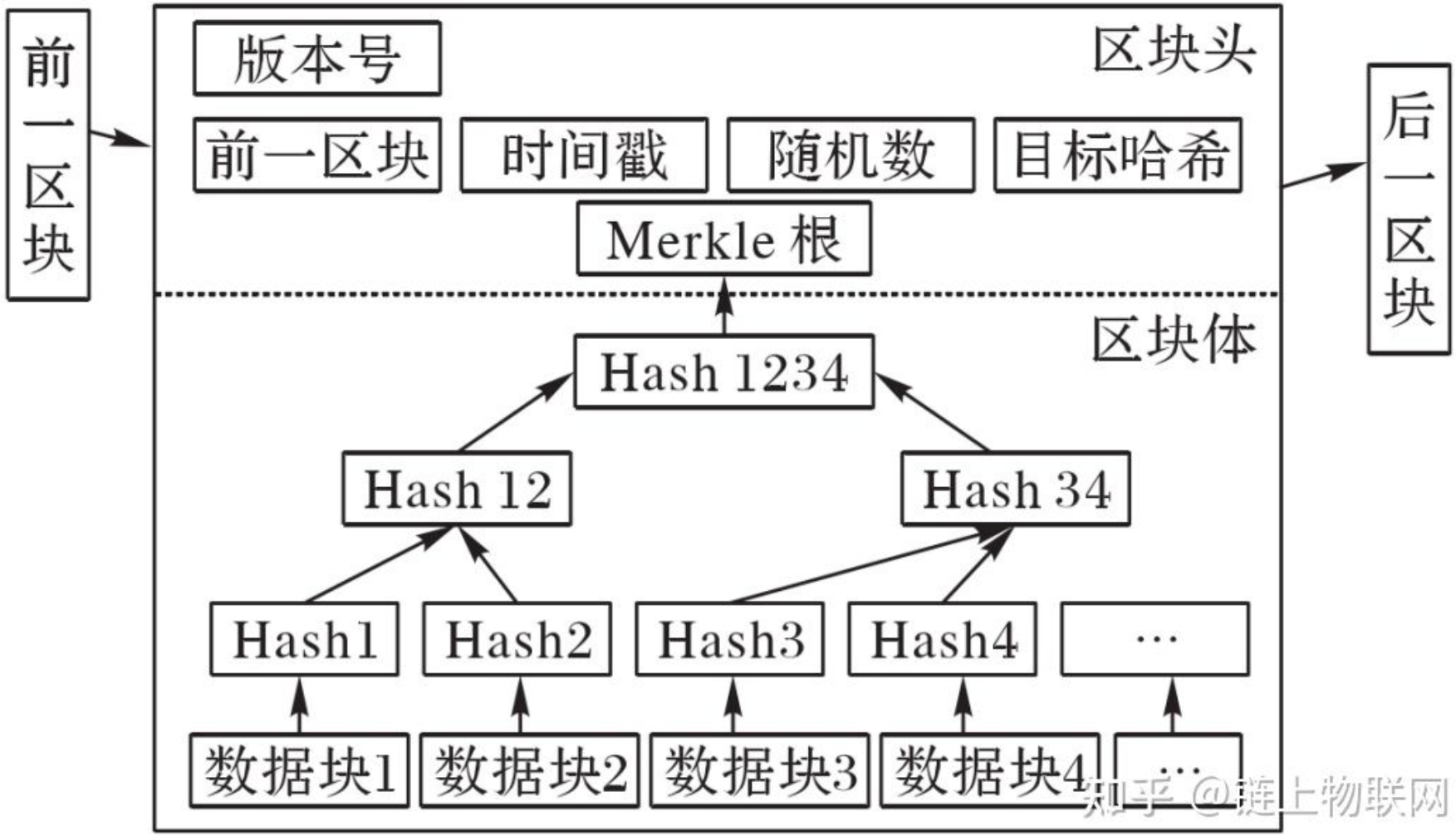
难度：难度不是固定不变的，会随着网络现有算力的变化而自动调节

Nonce：挖矿所要达到的目标值

区块体：一定时间内所生成的交易信息，即账本。

区块结构

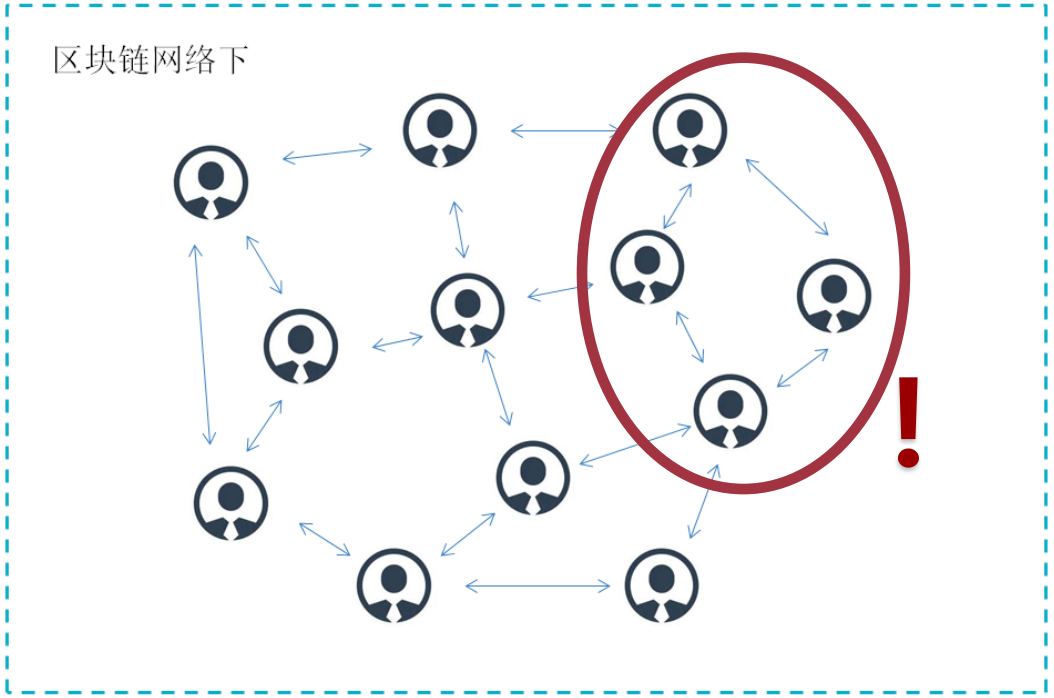
MORESHI POWERPOINT



网络层

MORESHI POWERPOINT

网络层，该层扮演着区块链网络中节点和节点之间信息交换的角色，负责用户点对点信息交换，它主要包括P2P(Peer-To-Peer network)网络机制、数据传播和验证机制。正是由于区块链的P2P特性，数据传输在节点之间进行，因此即使某些节点或网络被破坏，也不会对其他部分的传输产生影响。



共识层和激励层

MORESHI POWERPOINT

由于区块链中每个节点都可以生成新的区块完成记账，那要是所有节点同时都在记账，整个网络不就乱套了么？

共识层的功能是让高度分散的节点在P2P网络中，针对区块数据的有效性达成共识，决定了谁可以将新的区块添加到主链中。

目前已经出现了十余种共识机制算法，其中最为知名的有工作量证明机制（PoW）、权益证明机制（PoS）等。

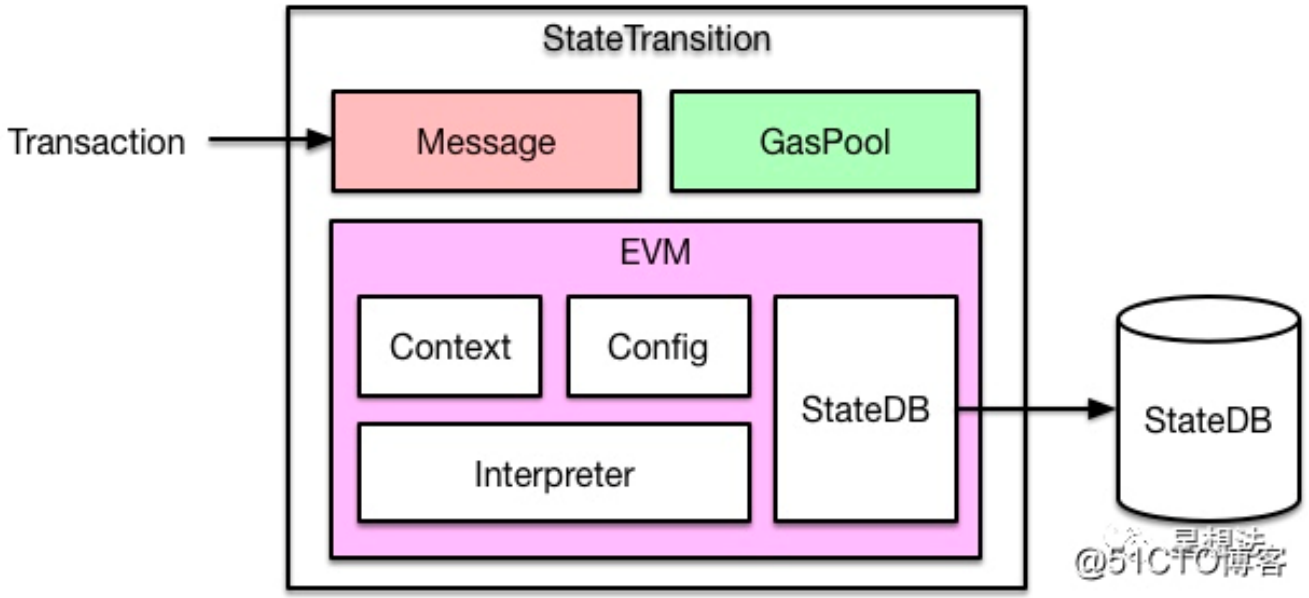
激励层的功能主要是提供一些激励措施，鼓励节点参与记账，保证整个网络的安全运行。通过共识机制胜出取得记账权的节点能获得一定的奖励。我们最熟悉的比特币的激励措施主要有两种，一种是新区块产生时系统奖励的比特币，另一种是每笔交易扣除的手续费。当比特币数量达到2100万枚的上限后，激励就全靠交易的手续费了。

合约层

MORESHI POWERPOINT

区块链具有可编程的特性，其基础是其合约层封装了各类脚本、算法和智能合约。比特币的脚本中就规定了比特币的交易方式和过程中的种种细节。

智能合约是存储在区块链上的一段代码，它们可以被区块链上的交易所触发，触发后，这段代码可以从区块链上读取数据或者向区块链上写入数据。这样就可以利用程序算法，替代人去仲裁和执行合约，将来将为我们节省巨额的信任成本。



应用层

MORESHI POWERPOINT

应用层封装了区块链的各种应用和场景，这个层面类似于电脑中的各种软件程序，是普通人可以真正直接使用的产品，也可以理解为B/S架构的产品中的浏览器端（Browser）。

典型应用示例有：

1. 热钱包
2. 区块链浏览器
3. 基于合约实现的Dapp
4. 中心化交易所

区块链交易以及上链流程

MORESHI POWERPOINT

那么当你按下“转账”按钮时，背后的区块链系统到底发生了什么?

1. 使用私钥对这笔即将发生的交易进行签名
2. 从你的客户端把你的这笔交易提交到区块链网络
3. 由已经开启“挖矿”程序的计算机（称为矿机）把10分钟内的交易打包成一个数据块（相当于一个账本，其中就包含了小明的这笔交易）
4. 这个数据块就包含在区块结构中的“区块体”，而此时，这些区块体中的交易并未生效。
5. 每个区块中都有一个哈希值，通过不断哈希运算，不断哈希运算（可能是几亿次）最终找到一个比当前哈希小的值，就认为这个区块被确认。即为交易生效，这个过程就称为“挖矿”。
6. 谁来做这个哈希？全球那么多交易，如果只是一家公司的几台计算机是远远不够的。所以，比特币有“激励机制”，当一台计算机确认了一个区块，就可以奖励12.5个比特币。为了得到报酬，越来越多矿工就有动力造更大更多算力的矿机来“挖矿”。越多的人参与挖矿的竞争，算力就越分散，比特币系统就越不可能被某一个人控制。

区块链简介

MORESHI POWERPOINT

每个人拥有同一个账本，即使你篡改了你自己的账本，让你的账上多了1亿，可是51%以上的账本中你的账户还是1分钱，那就说明你的帐上余额就是1分钱，无法抵赖。

去中心化，没有第三方中介，一切都由程序来完成。
安全性，主要体现在分布式、51%攻击，即使一个节点被攻击或宕机也不会影响网络的运行。

经济学与算力的保证：POW机制，抗51%算力攻击

在区块链的世界里，所有人的“账号”概念本质是“公钥”，“口令”即是“私钥”，私钥是证明身份的凭证。**因此账号的产生是离线的，几乎没有代价的。**

公链发展

MORESHI POWERPOINT

第一代区块链：比特币。POW机制，UTXO体系，简单的比特币脚本， “资产密码箱”

第二代区块链：以太坊。POW，账户体系，可编程， “具有可靠数据库的程序运行环境”

第三代区块链：其他创新公链。POS机制、DPOS机制，夜影协议，二层网络等...

区块链应用架构

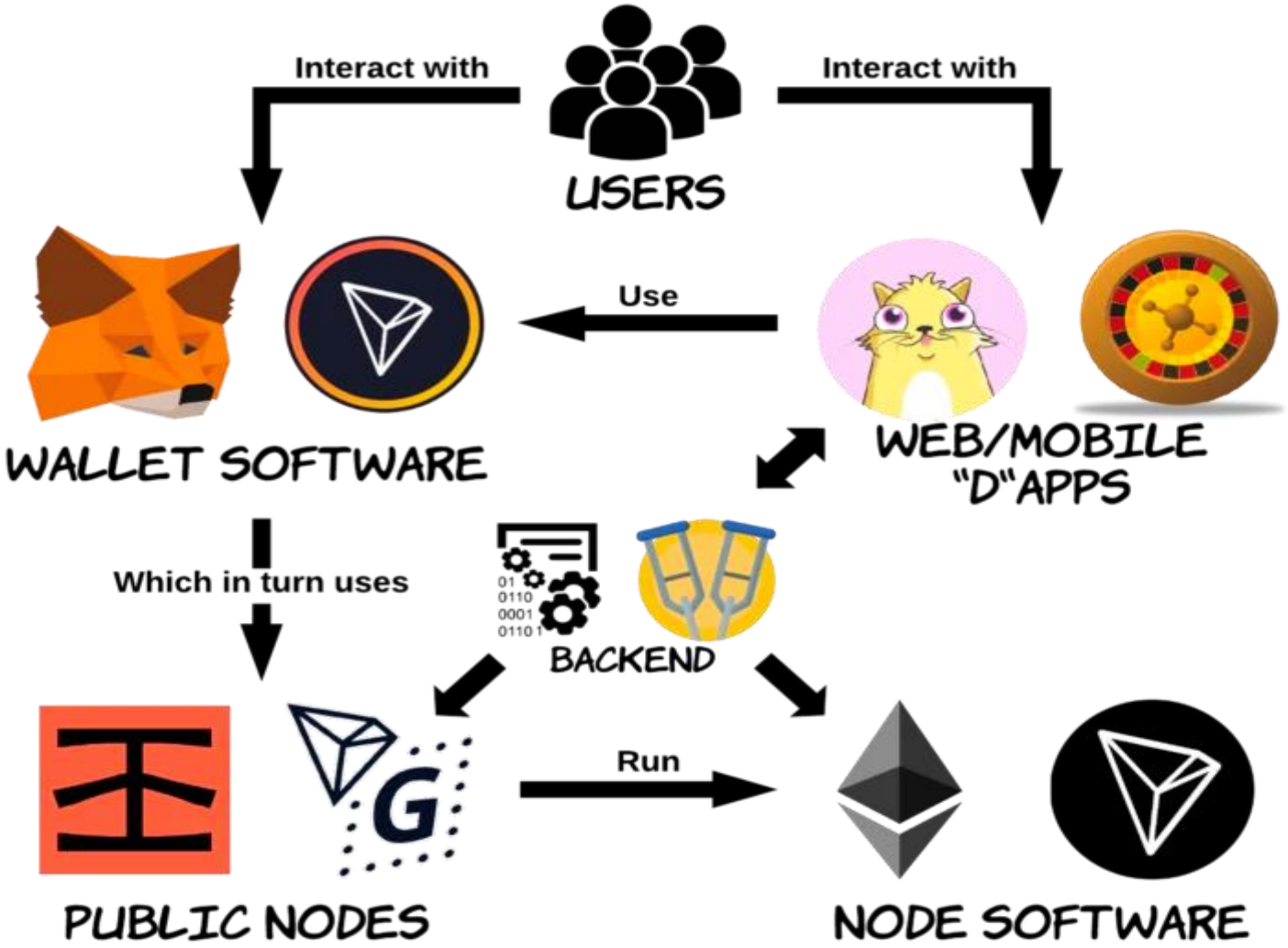
MORESHI POWERPOINT

应用分类，按类型分：

1. 热钱包
2. 区块链浏览器
3. 基于合约实现的Dapp
4. 中心化交易所

按照架构分：

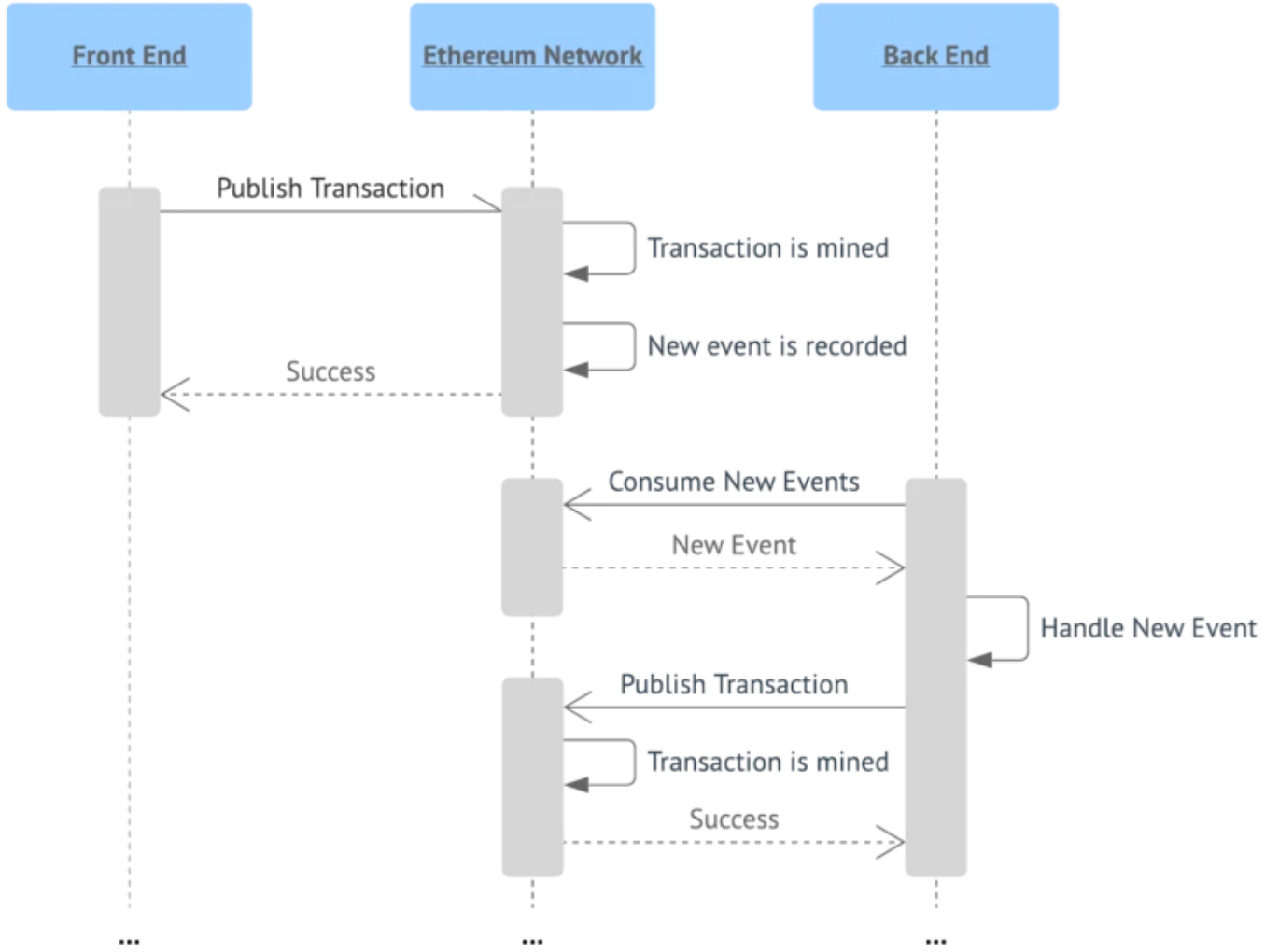
1. 前端-区块链 型
2. 前端-后端-区块链 型



思考：想要获取区块链数据怎么办?

区块链应用

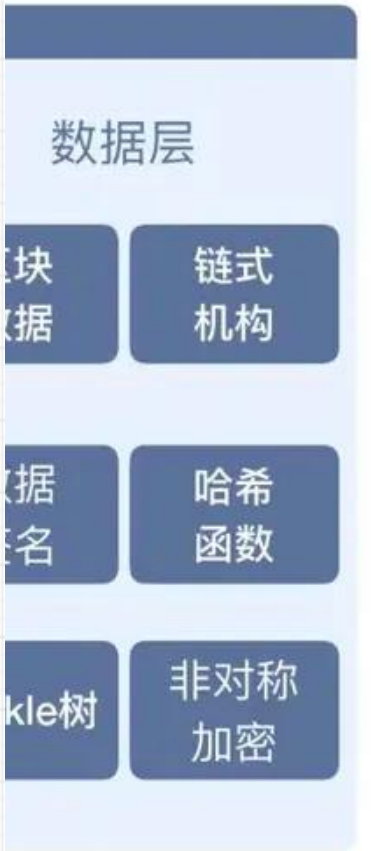
MORESHI POWERPOINT



区块链世界的安全风险

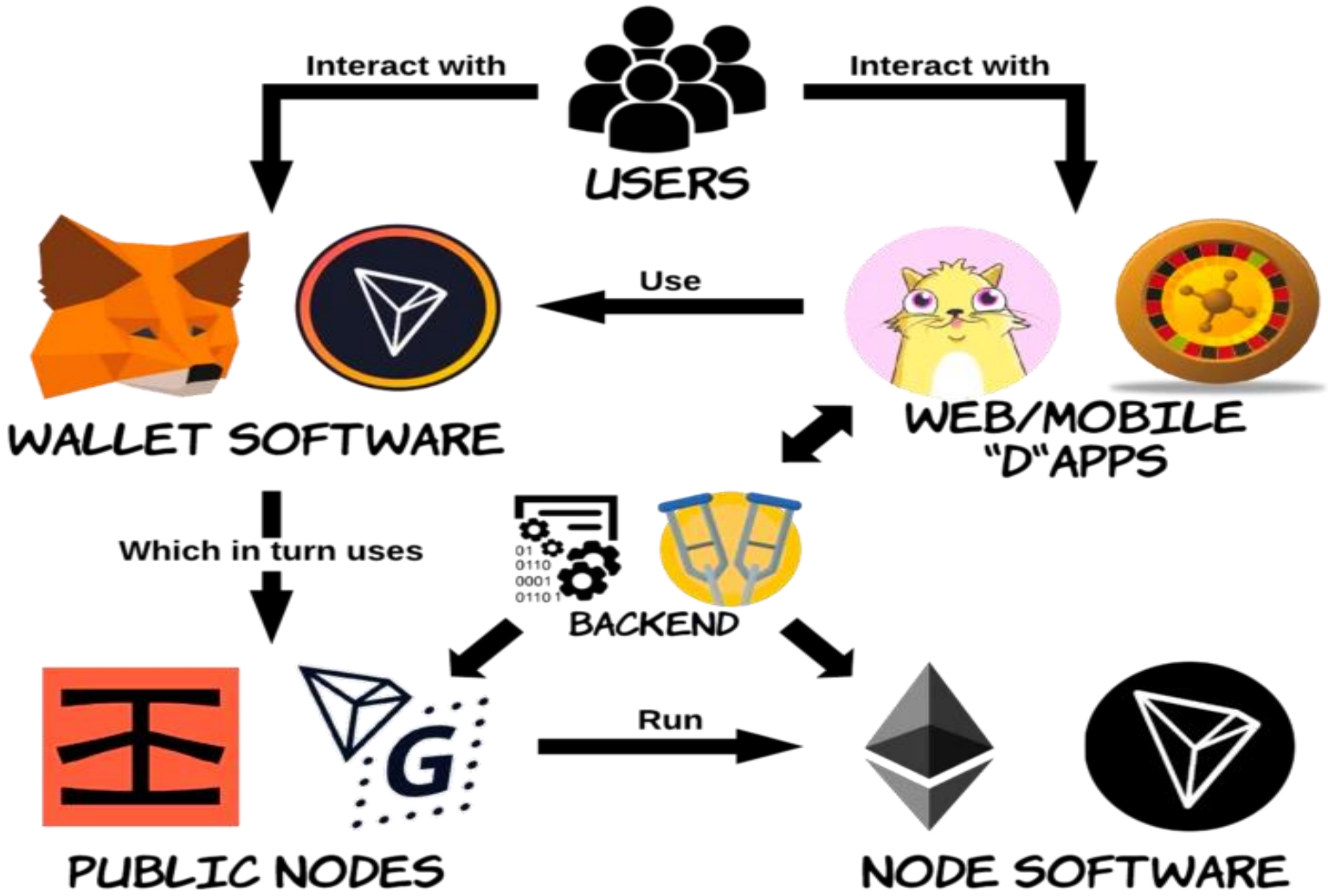
MORESHI POWERPOINT

应用层	交易所、矿机、矿池、钱包等业务攻击风险
合约层	智能合约漏洞、合约虚拟机漏洞等
激励层	算力下降导致攻击成本降低等
共识层	共识协议攻击（51%攻击）等
网络层	ddos攻击、日食攻击等
数据层	异形攻击、秘钥泄露等



区块链世界的安全风险

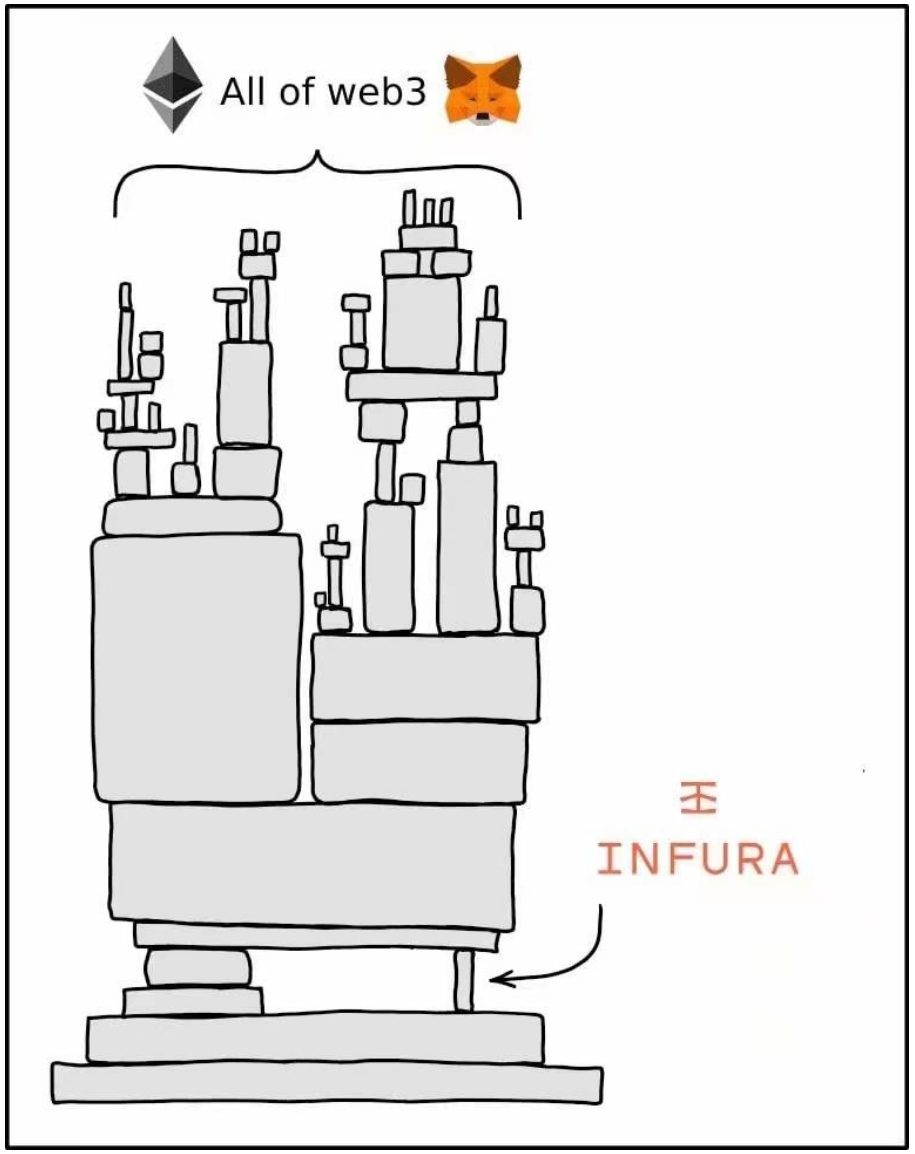
MORESHI POWERPOINT



区块链世界的安全风险

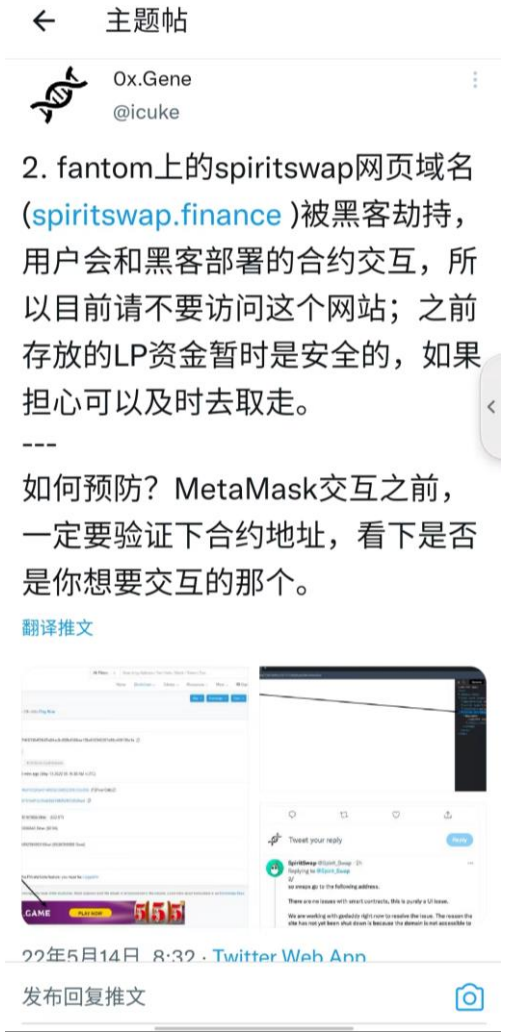
MORESHI POWERPOINT

1. 去中心化应用本身的安全缺陷，代码漏洞
2. 后端服务的可靠性风险
3. 基础节点服务的可靠性风险
4. 社会工程学风险（钓鱼邮件欺诈网站等）



🤔一些奇怪的安全风险源

MORESHI POWERPOINT

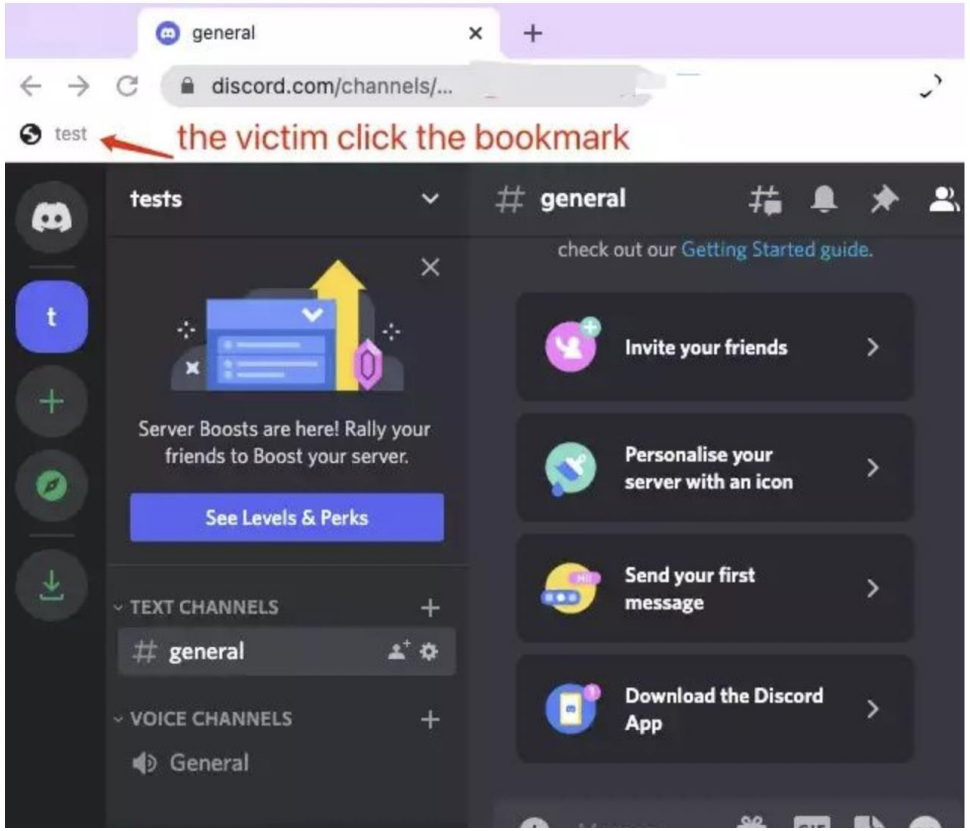


🤔一些奇怪的安全风险源

MORESHI POWERPOINT

演示采用的谷歌浏览器，在用户登录Web 端Discord 的前提下，假设受害者在钓鱼页面的指引下添加了恶意书签，在Discord Web 端登录时，点击了该书签，触发恶意代码，受害者的Token 等个人信息便会通过攻击者设置好的Discord webhook 发送到攻击者的频道上。

下面是演示受害者点击了钓鱼的书签：



区块链创新方向（学术创新、工程实践创新）

MORESHI POWERPOINT

围绕架构进行创新

区块链创新方向（学术创新、工程实践创新）

MORESHI POWERPOINT

合约层：

虚拟机的改进（并行执行、体系结构的创新等）

合约语言的演化

新型漏洞的检测

恶意交易的检测

激励和共识层：

共识机制的创新

共识漏洞的建模与分析

区块链创新方向（学术创新、工程实践创新）

MORESHI POWERPOINT

网络层：

抗日食攻击的新型组网机制等

数据层：

基于账户体系的创新

区块数据的隐私与加密

更小的区块数据结构设计

应用层：

应用创新

应用架构创新（TEE、Tor）

区块链创新方向

MORESHI POWERPOINT

围绕目前业界问题进行创新

针对扩容，区块链性能低下问题：

分片技术，例如Near链的夜影协议

侧链技术、Plasma技术，例如Polygon二层网络

rollup扩容方案，例如Arbitrum、optimism、zksync等

基于底层协议的创新，例如solana、flow、conflux

针对隐私交易保护问题：

隐私保护的链，例如Dash、Monero、Zcash

隐私保护的合约，例如Tornado

区块链创新方向（学术创新、工程实践创新）

MORESHI POWERPOINT

能不能让专门的合约数据在专门的链上：

合约链、交易链的划分

ERC20代币不一致问题：

新型的ERC20代币标准和形式

合约升级问题：

可升级合约标准

基于链增加合约升级的机制

未来量子计算机的攻击问题：

采用抗量子密码